

RECEIVED

JUL 8 - 2016

AT 8:30  
20160708/DS M

WILLIAM T. WALSH, CLERK UNITED STATES DISTRICT COURT  
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Criminal No. 15-626 (WJM)
	:	
v.	:	18 U.S.C. § 371
	:	18 U.S.C. § 1037
TIMOTHY LIVINGSTON,	:	18 U.S.C. § 1030
a/k/a "Mark Loyd"	:	18 U.S.C. § 1029
	:	18 U.S.C. § 1028A

**SUPERSEDING INDICTMENT**

The Grand Jury in and for the District of New Jersey, sitting at Newark,  
charges:

**COUNT ONE**

**(Conspiracy to Commit Fraud and Related  
Activity in Connection with Computers and Access Devices)**

1. At all times relevant to this Superseding Indictment:

**Relevant Individuals and Entity**

a. Defendant TIMOTHY LIVINGSTON, a/k/a "Mark Loyd," resided in or around Fort Lauderdale, Florida, and was the sole owner of a company that transmitted unsolicited electronic mail messages ("emails") in bulk, the primary purpose of which was the commercial advertisement or promotion of a commercial product or service (known as "spam" or "spam emails"). Defendant received payments in exchange for sending spam emails, including payments of at least \$5,000 in each of calendar years 2012, 2013, and 2014.

b. Tomasz Chmielarz resided in or around Clifton, New Jersey, and was a computer programmer. Among other things, Chmielarz authored hacking tools and other computer code used to facilitate the conduct described herein.

c. "Corporate Victim #1" was a telecommunications company headquartered in New York that, among other things, provided email services to its customers.

**The Conspiracy**

2. From in or about August 2012 through in or about March 2014, in Passaic County, in the District of New Jersey, and elsewhere, Defendant

**TIMOTHY LIVINGSTON,  
a/k/a "Mark Loyd,"**

did knowingly and intentionally conspire and agree with Tomasz Chmielarz and others to commit offenses against the United States, that is:

a. to knowingly and with intent to defraud access a protected computer without authorization and by means of such conduct further the intended fraud and obtain something of value, including the use of the computer, and the value of such use was more than \$5,000 within a 1-year time period, contrary to Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A);

b. to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, thus causing loss

to persons during a 1-year period from Defendant's course of conduct affecting protected computers aggregating at least \$5,000 in value, and damage affecting 10 or more protected computers during a 1-year period, contrary to Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(A)(i)(VI), and (c)(4)(B); and

c. to knowingly and with intent to defraud use and traffic in unauthorized access devices in a manner affecting interstate and foreign commerce, and by such conduct obtain \$1,000 or more during a 1-year period, contrary to Title 18, United States Code, Sections 1029(a)(2) and (c)(1)(a)(i).

### **Object of the Conspiracy**

3. The object of the conspiracy was for Defendant, Chmielarz, and others to enrich themselves by: (a) obtaining access credentials for email accounts housed on Corporate Victim #1's servers and used and controlled by its customers (the "Victim User Email Accounts"), without the authorization of Corporate Victim #1 or its customers; (b) damaging and accessing with the intent to defraud the Victim User Email Accounts without authorization; and (c) using the Victim User Email Accounts without authorization to transmit spam emails for private financial gain.

### **Manner and Means of the Conspiracy**

4. It was part of the conspiracy that from in or about August 2012 through in or about March 2014, Defendant and Chmielarz, together with others: (a) obtained without authorization the access credentials (i.e., user

names and passwords) for numerous Victim User Email Accounts; (b) hacked into and erased content within these Victim User Email Accounts; and (c) used these Victim User Email Accounts to transmit spam.

5. It was further part of the conspiracy that, at Defendant's direction and for Defendant's use, Chmielarz authored computer code designed to access Victim User Email Accounts without authorization (the "Email Account Software"). Once Defendant and Chmielarz used the Email Account Software to gain access to a Victim User Email Account, they would use the Email Account Software to delete content in the Victim User Email Account and use the account to transmit spam, all without authorization. The Email Account Software could also gain access to a Victim User Email Account, then create sub-accounts on the account and utilize those sub-accounts to transmit spam, all without authorization.

6. It was further part of the conspiracy that Defendant transmitted to Chmielarz certain access credentials for Victim User Email Accounts that were housed on Corporate Victim #1's servers. Chmielarz then used these credentials to test the Email Account Software.

7. It was further part of the conspiracy that Defendant used the Email Account Software to access and delete content within numerous Victim User Email Accounts without authorization, and then used these Victim User Email Accounts without authorization to transmit spam emails.

**Overt Acts**

8. In furtherance of the conspiracy and to effect its unlawful object, Defendant, Chmielarz, and others committed and caused to be committed the following overt acts, among others, in the District of New Jersey and elsewhere:

- a. In or about September and October 2012, Defendant and Chmielarz transmitted and received online messages in New Jersey discussing the creation and modification of versions of the Email Account Software.
- b. In or about September and October 2012, Chmielarz tested the Email Account Software from his computer in New Jersey.
- c. In or about September and October 2012, Defendant received versions of the Email Account Software transmitted from Chmielarz's computer in New Jersey.
- d. In or about September and October 2012, Defendant used the Email Account Software to send spam emails.
- e. On or about September 19, 2012, Defendant initiated, via an online payment system, a transfer of approximately \$1,500 to Chmielarz, who logged into his online payment account from New Jersey on or about that same date.

All in violation of Title 18, United States Code, Section 371.

**COUNT TWO**

**(Conspiracy to Commit Fraud and Related Activity in Connection with Electronic Mail)**

1. The allegations contained in paragraphs 1 and 4 through 8 of Count One of this Superseding Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. At all times relevant to this Superseding Indictment:

**Additional Relevant Entity**

a. “Corporate Victim #2” was a technology and consulting company headquartered in New York.

**Relevant Terms**

b. A “domain name” was any alphanumeric designation which was registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet.

c. A “hyperlink” was an element in a document (e.g., an email or a World Wide Web page) that linked to another location on the Internet, often a World Wide Web page.

d. “Header information” was the source, destination, and routing information attached to an email, including the originating domain name and originating email address, and any other information that appeared in the line identifying, or purporting to identify, a person initiating the email.

e. “Proxy servers” were computers that accepted incoming connections from a computer and then made outgoing connections to other computers. Proxy servers could be used by spammers to camouflage the originating IP address of a connection to a computer.

f. “Spam filters” were tools used by Internet service providers that were designed to prevent spam from reaching their customers’ email accounts.

### **The Conspiracy**

3. From at least as early as in or about January 2012 through in or about September 2015, in Passaic County, in the District of New Jersey, and elsewhere, Defendant

**TIMOTHY LIVINGSTON,  
a/k/a “Mark Loyd,”**

did knowingly and intentionally conspire and agree with Tomasz Chmielarz and others to: (a) knowingly access a protected computer without authorization and intentionally initiate the transmission of multiple commercial electronic mail messages from and through such computer; (b) knowingly materially falsify header information in multiple commercial electronic mail messages and intentionally initiate the transmission of such messages; and (c) knowingly register, using information materially falsifying the identity of the actual registrant, for five or more electronic mail accounts and online user accounts and two or more domain names, and intentionally initiate the transmission of



multiple commercial electronic mail messages from a combination of such accounts and domain names, under the circumstances described in Paragraph 11 of this Count.

**Object of the Conspiracy**

4. The object of the conspiracy was for Defendant, Chmielarz, and others to enrich themselves by: (a) accessing the email accounts of Corporate Victim #1's customers without authorization; (b) leveraging vulnerabilities in the websites of a number of corporations, including Corporate Victim #2; (c) using these email accounts and websites without authorization, and other means, to transmit spam emails for private financial gain; and (d) concealing the true origin of the emails, evading security measures and spam filters, and deceiving and misleading recipients and Internet service providers as to the origin of the spam emails that were transmitted.

**Manner and Means of the Conspiracy**

5. It was part of the conspiracy that beginning in or about January 2012, Defendant directed Chmielarz to write computer code for Defendant's use to transmit spam emails in a manner that concealed the true origin of the emails, evaded security measures and spam filters, and deceived and misled recipients and Internet service providers as to the origin of spam emails that were transmitted.

6. It was further part of the conspiracy that Defendant used various



pieces of computer code authored by Chmielarz to access the servers of Corporate Victim #1, Corporate Victim #2, and other corporations through proxy servers to send spam emails. One piece of code that included this functionality was the Email Account Software.

7. It was further part of the conspiracy that, at Defendant's direction, Chmielarz authored code that leveraged vulnerabilities in the websites of a number of corporations, including Corporate Victim #2 (the "Web Form Software"). The Web Form Software allowed Defendant and Chmielarz to access the servers of victim corporations, including Corporate Victim #2, in order to transmit spam emails that appeared to originate from the victim corporations.

8. It was further part of the conspiracy that Defendant and Chmielarz created and modified a version of the Web Form Software to enter commands into user-submitted forms on Corporate Victim #2's websites. Those commands directed Corporate Victim #2's servers to transmit spam emails in an unauthorized manner.

9. It was further part of the conspiracy that Defendant, Chmielarz, and others used a variety of techniques in the transmission of the spam emails, including the material falsification of header information, the use of proxy servers, and the masking of hyperlinks. These techniques were employed to conceal the true origin of the emails, evade security measures and spam filters, and deceive and mislead recipients and Internet service providers as to the origin

of spam emails that were transmitted.

10. It was further part of the conspiracy that using these and other techniques and means, Defendant transmitted large amounts of spam emails that misled recipients and Internet access providers as to the true origin of the messages.

11. It was further part of the conspiracy that, using these and other techniques and means, (a) Defendant accessed a protected computer without authorization, and intentionally initiated the transmission of multiple commercial electronic mail messages from or through such computer; (b) the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during a 24-hour period, 25,000 during a 30-day period, and 250,000 during a 1-year period; (c) the offense caused loss to one or more persons aggregating \$5,000 or more in value during a 1-year period; and (d) as a result of the offense Defendant obtained something of value aggregating \$5,000 or more during a 1-year period.

All in violation of Title 18, United States Code, Sections 1037(a)(1), 1037(a)(3), 1037(a)(4), 1037(b)(2)(A), 1037(b)(2)(C), 1037(b)(2)(D), and 1037(b)(2)(E).

**COUNT THREE**  
**(Accessing a Computer in Furtherance of Fraud)**

1. The allegations contained in paragraphs 1 and 4 through 8 of Count One and paragraphs 2 and 5 through 11 of Count Two of this Superseding Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. In or about October 2012, in Passaic County, in the District of New Jersey, and elsewhere, Defendant

**TIMOTHY LIVINGSTON,**  
**a/k/a “Mark Loyd,”**

knowingly and with intent to defraud accessed a protected computer without authorization and by means of such conduct furthered the intended fraud and obtained something of value, including the use of the computer, and the value of such use was more than \$5,000 within a 1-year time period.

In violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A), and 2.

**COUNT FOUR**  
**(Intentionally Damaging a Computer by Knowing Transmission  
of a Program, Information, Code, or Command)**

1. The allegations contained in paragraphs 1 and 4 through 8 of Count One and paragraphs 2 and 5 through 11 of Count Two of this Superseding Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. In or about October 2012, in Passaic County, in the District of New Jersey, and elsewhere, Defendant

**TIMOTHY LIVINGSTON,  
a/k/a "Mark Loyd,"**

knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, and the offense caused loss to persons during a 1-year period from Defendant's course of conduct affecting protected computers aggregating at least \$5,000 in value, and damage affecting 10 or more protected computers during a 1-year period.

In violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B), and 2.

**COUNT FIVE**  
**(Using or Trafficking in an Unauthorized Access Device)**

1. The allegations contained in paragraphs 1 and 4 through 8 of Count One and paragraphs 2 and 5 through 11 of Count Two of this Superseding Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. On or about October 24, 2012, in Passaic County, in the District of New Jersey, and elsewhere, Defendant

**TIMOTHY LIVINGSTON,**  
**a/k/a "Mark Loyd,"**

knowingly and with intent to defraud, used and trafficked in unauthorized access devices in a manner affecting interstate and foreign commerce, to wit, usernames and passwords for email accounts hosted by Corporate Victim #1, and by such conduct obtained \$1,000 or more during a 1-year period.

In violation of Title 18, United States Code, Sections 1029(a)(2) and (c)(1)(a)(i), and 2.

**COUNT SIX**  
**(Aggravated Identity Theft)**

1. The allegations contained in paragraphs 1 and 4 through 8 of Count One and paragraphs 2 and 5 through 11 of Count Two of this Superseding Indictment are re-alleged and incorporated as though fully set forth in this paragraph.

2. On or about October 24, 2012, in Passaic County, in the District of New Jersey, and elsewhere, Defendant

**TIMOTHY LIVINGSTON,**  
**a/k/a "Mark Loyd,"**

did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, to wit, usernames and passwords for email accounts hosted by Corporate Victim #1, during and in relation to felony violations enumerated in Title 18, United States Code, Section 1028A(c), to wit, violations of Title 18, United States Code, Sections 1029, 1030, and 1037, knowing that the means of identification belonged to another actual person.

In violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

**FORFEITURE ALLEGATION AS TO  
COUNTS ONE, THREE, AND FOUR**

1. Upon conviction of the violations of and conspiracy to violate 18 U.S.C. § 1030 alleged in Counts One, Three, and Four of this Superseding Indictment, Defendant TIMOTHY LIVINGSTON shall forfeit to the United States:

- a. pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of the offense charged in each such count; and
- b. pursuant to 18 U.S.C. § 1030(i), all right, title, and interest of Defendant in any personal property that was used or intended to be used to commit or to facilitate the commission of the offense charged in each such count, including, but not limited to, all right, title, and interest of the defendant in the following:

- (i) The contents of Scottrade Inc. account number ending in 8422 held in the name of Timothy E. Livingston, which was seized pursuant to a seizure warrant on or about July 27, 2015;
- (ii) The contents of Wells Fargo account number ending in 6185 held in the name of Timothy Livingston, which was seized pursuant to a seizure warrant on or about July 27, 2015;
- (iii) The contents of Wells Fargo account number ending in 4593 held in the name of A Whole Lot of Nothing, LLC, which was seized pursuant to a seizure warrant on or about July 27, 2015;
- (iv) The contents of Wells Fargo account number ending in 9783 held in the name of A Whole Lot of Nothing, LLC, which was seized pursuant to a seizure warrant on or about July 27, 2015;



- (v) The contents of Wells Fargo account number ending in 9855 held in the name of Timothy Livingston, which was seized pursuant to a seizure warrant on or about July 27, 2015;
- (vi) One 2009 Cadillac Escalade, which was seized pursuant to a seizure warrant on or about July 27, 2015;
- (vii) One 2006 Ferrari F430 Spider, which was seized pursuant to a seizure warrant on or about July 27, 2015; and
- (viii) All the computers, media storage devices, mobile phones and tablets that were seized pursuant to search warrant on or about July 27, 2015 and on or about December 15, 2015 .

and all property traceable to such property (hereinafter referred to collectively as the "Specific Properties").

**FORFEITURE ALLEGATION AS TO COUNT TWO**

2. As a result of committing the offense alleged in Count Two of this Superseding Indictment, Defendant TIMOTHY LIVINGSTON shall forfeit to the United States, pursuant to 18 U.S.C. § 1037, all of Defendant's right, title, and interest in:

- a. any property, real or personal, constituting or traceable to gross proceeds obtained from such offense; and
- b. any equipment, software, and other technology used or intended to be used to commit or to facilitate the commission of such offense; including, but not limited to, all right, title, and interest of Defendant in the Specific Properties.

**FORFEITURE ALLEGATION AS TO COUNTS ONE AND FIVE**

3. As a result of committing the violations of and conspiracy to violate 18 U.S.C. § 1029 alleged in Counts One and Five of this Superseding Indictment, Defendant TIMOTHY LIVINGSTON shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(2)(B), any property constituting, or derived from, proceeds obtained directly or indirectly, as a result of such offenses, including, but not limited to all right, title, and interest of Defendant in the Specific Properties.

**SUBSTITUTE ASSETS PROVISION**  
**(Applicable to All Forfeiture Allegations)**


4. If any of the above-described forfeitable property, as a result of any act or omission of Defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

the United States shall be entitled, pursuant to 21 U.S.C. § 853(p) (as incorporated by 28 U.S.C. § 2461(c), 18 U.S.C. § 1030(i), and 18 U.S.C. § 982(b)), to forfeiture of any other property of Defendant up to the value of the above-described forfeitable property.

A TRUE BILL

\_\_\_\_\_  
FOREPERSON

  
\_\_\_\_\_  
PAUL J. FISHMAN  
UNITED STATES ATTORNEY

CASE NUMBER: 15-626 (WJM)

United States District Court  
District of New Jersey

UNITED STATES OF AMERICA

v.

TIMOTHY LIVINGSTON,  
a/k/a "Mark Loyd"

SUPERSEDING INDICTMENT FOR

18 U.S.C. § 371  
18 U.S.C. § 1037  
18 U.S.C. § 1030  
18 U.S.C. § 1029  
18 U.S.C. § 1028A

PAUL J. FISHMAN  
U.S. ATTORNEY  
NEWARK, NEW JERSEY

ASSISTANT U.S. ATTORNEY  
DANIEL SHAPIRO  
(973) 353-6087

DOJ/CCIPS TRIAL ATTORNEY  
WILLIAM HALL

USA-48AD 8  
(Ed. 1/97)